The following is a complete listing of all claims in the application, with an indication of the status of each.

Listing of claims:

1. (currently amended)

A system for providing private messaging among multiple users without requiring users to exchange encryption/authentication certificates with one another either directly or indirectly, comprising:

a packet network;

one or more private messaging agents coupled to the packet network, wherein the private messaging agents handle private messages and corresponding access restrictions messages;

one or more trusted couriers coupled to the packet network and operable to relay the private messages and corresponding access restrictions messages between the private messaging agents, wherein the one or more trusted couriers operate to convey private messages independently from corresponding access restrictions messages.

2. (currently amended)

The system of claim 1 in which each trusted courier comprises:

a foreground element operable to transfer private messages among the private messaging agents registered to it, as well as between itself and other trusted courier foreground elements, and to communicate encryption/authentication certificates without user involvement between itself and private messaging agents registered to it, as well as between itself and other trusted courier foreground elements; and

a background element operable to transfer ~~the~~ access restrictions messages and other background signaling among the private messaging agents registered to it, as well as between itself and other trusted courier background elements, and to communicate

encryption/authentication certificates without user involvement between itself and private messaging agents registered to it, as well as between itself and other trusted courier background elements;

wherein the foreground and background elements operate to transfer private messages independently from corresponding access restrictions messages.

3. (cancelled)

4. (cancelled)

5. (cancelled)

6. (currently amended)

The system of claim 1 in which at least one trusted courier is configured to serve multiple users without any constraint on the domain of their addresses, and is operable to reconcile a rejection that it may receive from an existing private messaging agent when inviting a user to register.

7. (currently amended)

The system of claim 1 in which at least one trusted courier is a private courier that may serve only users whose address is within the same domain as the trusted courier, and is operable to defer invitations for users outside its domain to a superior courier.

8. (cancelled)

9. (cancelled)

10. (currently amended)

A trusted courier comprising:

a foreground element operable to transfer private messages ~~to external~~ among private messaging agents registered to it, as well as between itself and other trusted courier foreground elements, and to communicate encryption/authentication certificates

without user involvement between itself and private messaging agents registered to it, as well as between itself and other trusted courier foreground elements; and

a background element operable to transfer access restrictions messages ~~to external~~ among private messaging agents registered to it, as well as between itself and other trusted courier background elements, and to communicate encryption/authentication certificates without user involvement between itself and private messaging agents registered to it, as well as between itself and other trusted courier background elements;

wherein the foreground and background elements operate to transfer private messages independently from corresponding access restrictions messages.

11. (cancelled)

12. (cancelled)

13. (cancelled)

14. (currently amended)

A method of providing private messaging services comprising:

sending an Invitation to Register to a prospective user of the private messaging service;

subsequently registering a user by establishing an account and automatically providing an agent with ~~key materials~~ encryption/authentication certificates for the prospective user;

routing the ~~key material~~ content keys and access restrictions associated with each private message between registered users through the background element of one or more trusted couriers separately from the private messages; and

routing the private messages between registered users through the foreground element of one or more trusted couriers, separately from the content keys and access restrictions.

15. (cancelled)

16. (currently amended)

A method in accordance with claim 14 wherein the act of establishing an account ~~comprises~~ includes:

~~presenting a form to the prospective new user containing the messaging address to which Invitation had been sent;~~

~~requesting an account password for service access control, user contact information, and billing information;~~

downloading an Agent installer application program which installs a private messaging Agent to the prospective new user's computer;

subsequently executing the Agent installer to install the Agent in such a manner that it will persist and manage all future private messages, corresponding content keys, and corresponding access restrictions on behalf of the user;

~~establishing a local password for ensuring that future access to the agent may only be accomplished by the new user;~~ and

creating and exchanging between the agent and a single designated trusted courier a number of ~~cryptographic keys;~~ encryption/authentication certificates.

~~storing the keys;~~

~~sending an indication that the agent is installed correctly to the trusted courier;~~ and

~~activating the newly registered user's account in the trusted courier.~~

17. (currently amended)

A method in accordance with claim 16 further comprising the acts of:

propagating the newly registered user's account, including all ~~keys~~ encryption/authentication certificates, from the foreground element of said single designated courier to its corresponding background element.

18. (previously presented)

A private messaging system implementing the method of claim 14.

19. (currently amended)

A private messaging system for routing a message between a first agent and a second agent without requiring said agents to exchange encryption/authentication certificates with one another either directly or indirectly, the system comprising:

a first courier having a trust relationship with the first agent;

a second courier having a trust relationship with the second agent and with the first courier;

wherein the first courier is operable to receive a message identifying the second agent as a recipient from the first agent, determine that the second agent has a trust relationship with the second courier, and send the message to the second courier using the trust relationship between the first courier and the second courier; and

wherein the second courier is operable to relay the message to the second agent using the trust relationship between the second courier and the second agent.

20. (currently amended)

The private messaging system of claim 19 wherein at least a portion of the message is encrypted by the first ~~courier~~ agent using a content encryption key (CEK); and
the CEK is conveyed to the second agent ~~using a communication channel~~ separate from ~~a communication channel used to send and relay~~ the message.

21. (cancelled)

22. (cancelled)

23. (cancelled)

24. (currently amended)

A method for routing a private message between a sending agent and a recipient agent, the method comprising:

providing a first agent;

~~providing a second agent;~~

~~providing~~ and a first courier having knowledge of a number of agents, including the first agent, that are registered with the first courier;

providing a second agent and a second courier having knowledge of a number of agents, including the second agent, that are registered with the second courier;

subsequently providing a private message from the first agent to the first courier, the private message comprising a header and a message ID, wherein the private message header identifies a recipient address of the second agent, and wherein the content is encrypted using a content encryption key (CEK);

next signing and encrypting the private message with a first message signing key used by the first agent for messages to the first courier;

then sending the signed private message in one or more parts, ~~the signed private message~~ addressed to the first courier, the message comprising the header, message ID, the encrypted content of the private message, and the CEK used to encrypt the content of the private message;

upon arrival of the aforementioned signed private message in the first courier, decrypting and validating the private message header using the first message signing key known to the first courier, wherein the private message content remains encrypted by the CEK;

next identifying the second courier from the recipient address in the decrypted first message header;

then for each of the at least one registered recipient addresses in the decrypted message header, reconstructing the message and relaying it by:;

first signing and encrypting the reconstructed message using a second message signing key used by the first courier for messages to the second courier;

then sending the signed and encrypted reconstructed message in one or more parts to the second courier, the signed and encrypted reconstructed message comprising the header, message ID, the encrypted content of the private message, and the CEK used to encrypt the content of the private message;

upon arrival of the aforementioned signed and encrypted reconstructed message in the second courier, decrypting and validating the private message header using the second message signing key known to the second courier, wherein the private message content remain encrypted by the CEK;

next identifying the recipient address in the decrypted message header;

then signing and encrypting the private message with a third message signing key used by the second agent for messages to the second agent; and

sending the signed private message in one or more parts to the second agent, the message comprising the header, message ID, the encrypted content of the private message, and the CEK used to encrypt the content of the private message;

upon arrival of ~~decrypting~~ the signed private message in the second agent, decrypting it using the third message signing key; and

decrypting the encrypted content in the second agent using the CEK.

25. (cancelled)

26. (cancelled)

27. (cancelled)

28. (currently amended)

The method of claim ~~27~~ 24 wherein the first courier comprises a foreground component and a background component and the second courier comprises a foreground component and a background component;

the act of sending the signed private message to the first courier comprises:

sending a foreground message part from the first agent to the foreground component of the first courier, wherein the foreground message part comprises a message body that contains the header, message ID, and CEK-encrypted content of the private message;

sending a background message part from the first agent to the background component of the first courier separately from the foreground message part, wherein the background message part comprises a message body that contains the header, message ID, and the CEK used to encrypt the content of the private message;

and the act of sending the signed and encrypted reconstructed message comprises:

sending a foreground message part from the first courier foreground component to the foreground component of the second courier, wherein the foreground message part

comprises a message body that contains the header, message ID, and CEK-encrypted content of the private message;

sending a background message part from the first courier background element to the background component of the first courier, wherein the background message part comprises a message body that comprises the header, message ID, and the CEK used to encrypt the content of the private message;

wherein the acts of sending the foreground and background message parts are performed ~~over separate, independent communication channels~~ in parallel, in such a manner that they are kept separate from one another and conveyed independently.